

Windows Hello for Business

Nicola Suter

-6-6:5050



About

Nicola Suter

Modern Workplace engineer for itnetX (Switzerland) AG

BSc student in computer sciences

Blog: tech.nicolonsky.ch

Twitter: <u>@nicolonsky</u>



Advantages over passwords

- Device based multi factor authentication
- Passwordless







Device state	User state	Effort
Azure AD Joined	Azure AD user	-
Azure AD Joined	Hybrid identity	++, +++
Hybrid Azure AD Joined	Hybrid identity	+, ++
Domain Joined	AD user	++++



Prerequisites

- Windows 10 1903 (introduced FIDO2 key sign-in)
- Azure Active Directory

Recommended prerequisites:

- TPM (if no TPM present, private key gets enrolled to software KSP \rightarrow less secure)
- Hardware with biometric support (IR camera, fingerprint)



Windows Hello for Business settings can be managed with:

• Group Policy

geekmania switzerland 2019

- Microsoft Intune (passportforwork-csp)
- Microsoft Endpoint Configuration Manager; deprecated

Microsoft 365 Device Manage	ement		ಧ 🍪 ? 😳 nicola@nicolasuter.ch 🌒
«	Home > Devices > Enroll devices - Win	dows enrollment	Windows Hello for Business ×
숨 Home 🗔 Dashboard	Enroll devices - Window	s enrollment	Window enrollment Last modified Assigned to 8/28/18, 213 PM All users.
All services All services Apps Conditional administration	Search (Ctrl+/) Windows enrollment Apple enrollment Android enrollment Enrollment restrictions Corporate device identifiers Device enrollment managers	Learn about the seven different ways a Windows 10 PC can be enrolled into Intune by users or admins. Learn more General Configure Windows devices to enroll when they join or register with Azure Active Directory. Windows Hello for Business Replace passwords with strong two-factor authentication.	Windows Hello for Business settings lets users access their devices using a gesture, such as biometric authentication, or a PIN. Learn more Configure settings for enrolled Windows 10, Windows 10 Mobile and later. Name All users and all devices Description This is the default Windows Hello for Business configuration applied with the lowest priority to all users recardless of group membership.
7 Troubleshooting + support		CNAME Validation Test company domain CNAME registration for Windows enrollment. Enrollment Status Page Show app and profile installation statuses to users during device setup.	
		Windows Autopilot Deployment Program	Configure Windows Hello for Business: O Not configured Use security keys for sign-in: O Not configured
	4	Configure hybrid Azure AD joined devices	Save Discard

Management tools - Intune

• Dedicated profile type: "identity protection"

geekmania switzerland 2019

• Overrides configured settings in device enrollment!

Windows Hello for Business Windows 10 and later	
Configure Windows Hello for Business: 🛈	Enable V
Minimum PIN length: ①	6
Maximum PIN length: ①	Not configured
Lowercase letters in PIN: ①	Allowed
Uppercase letters in PIN: ①	Allowed
Special characters in PIN: ①	Allowed 🗸
PIN expiration (days): ①	Not configured \checkmark
Remember PIN history: ①	Not configured \checkmark
Enable PIN recovery: 🛈	Enable Not configured
Use a Trusted Platform Module (TPM): 🛈	Enable Not configured
Allow biometric authentication: ①	Enable Not configured
Use enhanced anti-spoofing, when available: 🛈	Enable Not configured
Certificate for on-premise resources: ①	Enable Not configured
Use security keys for sign-in: ①	Enable Not configured

End user experience



TAB-W10-AAD-02 on X-011811282257 - Virtual Machine Connection

- 🗆 🗙

Your organization requires Windows Hello

What takes seconds to create and gives you fast and secure sign-in? A Windows Hello PIN! It only works on your device, so it stays off the web.





Status: Running



Multifactor unlock

- Require an additional factor to unlock a device
- Benefit as long as password sign-ins are still possible?

First unlock factor	Second unlock factor
PINFingerprintFacial Recognition	 PIN Trusted Signal Phone proximity Network location Wi-Fi network

a credential supported by that provider can **only satisfy one** of the unlock factors



Configuration with Intune policy CSP:





• Admin consent for Azure AD applications required!

PIN reset

geekmania switzerland 2019

Enterprise applications -	All applications		
«	+ New application Ell Columns		
Overview			
 Overview 	Application Type Applications status Application visibility	olv Reset	
🗙 Diagnose and solve problems	energine oppressions • Thy • Thy • Thy		
	Microsoft Pin		
Manage			
All applications		OBJECT ID	AFFLICATION ID
Application proxy	Microsoft Pin Reset Client Production	f3b9f2f7-ff88-422d-b2f9-ba327dc6945a	9115dd05-fad5-4f9c-acc7-305d08b1b04e
User settings	Microsoft Pin Reset Service Production https://cred.microsoft.com	3c97b323-46e4-46da-a761-f7c513e7cc15	b8456c59-1230-44c7-a4a2-99b085333e



.

Dynamic lock

- Automatically lock device screen when paired device moves
- Improves default value of 15 minutes for the screen lock
- Uses Bluetooth Received Signal Strength Indication (RSSI)
- Required signal strength can be overridden

\leftarrow Settings	
☆ Home Find a setting	Sign-in options
Accounts	ି
요프 Your info	Windows can use devices that are paired to your PC to know when you're away and lock your PC when those devices go out of range.
🖾 Email & accounts	Allow Windows to lock your device automatically when you're away
🔍 Sign-in options	
Access work or school	tech.nicolonsky.ch
A₊ Other users	Bluetooth & other devices Learn more
\mathcal{C} Sync your settings	



On premise resource access

🐂 📝 🔚 🖛 File Expl	orer		_	
File Home Share	e View			~ 🔮
← → ~ ↑ ♣ • Q	uick access 🗸 🗸	× P Search Quick access		
Quick access	V Frequent folders (6)	Doubloade		
Desktop	This PC	This PC		
Pictures *	Windows Security	X		
Videos This PC	Enter network credentia	als t to: intra.tech.nicolonsky.ch		
💣 Network	Email address			
	Password		s here.	
	Remember my credentials			
	The user name or password is inc	correct.		
	ОК	Cancel		
6 items				

The Security System detected an authentication error for the server Idap/ADDS01.intra.tech.nicolonsky.ch/intra.tech.nicolonsky.ch@INTRA.TECH.NICOLONSKY.CH. The failure code from authentication protocol Kerberos was "The revocation status of the domain controller certificate used for authentication could not be determined. There is additional information in the system event log. (0xc000040c)".

🌉 Enterprise Key Admins 👘

Remote Desktop Services Profile COM+ Attribute Editor General Address Account Profile Telephones Organizatic Published Certificates Member Of Password Replication Dial-in Obje Member of: Name Active Directory Domain Services Folder Domain Users intra tech nicolonsky.ch/Users Name Active Directory Domain Services Folder Domain Users intra tech nicolonsky.ch/Users Just intra tech nicolonsky.ch/Users intra tech nicolonsky.ch/Users Issaid Users intra tech nicolonsky.ch/Users Issaid Issaid Issaid Member Of Password Replication Dial-in Security Environment Sessions Remote Security Environment Sessions Remote Org	Address Account Profile COM+ Attribute Editor erral Address Account Profile Telephones Organization shed Certificates Member Of Password Replication Dial-in Object nber of: arme Active Directory Domain Services Folder Dial-in Object arme Active Directory Domain Services Folder Dial-in Object omain Users intra.tech.nicolonsky.ch/Users Dial-in Object arged Admins intra.tech.nicolonsky.ch/Users Environment Sessions Remote cor arged Admins intra.tech.nicolonsky.ch/Builtin Profile Telephones Organization icola Properties ? Profile Telephones Organization icola Properties ? Profile Telephones Organization icola Properties ? Profile Telephones Organization icola Properties Account Profile Telephones Organization imate Desktop Services Profile COM+ Attribute Editor Attribute Editor imate Desktop Services Profile	Security	Env	ironment	See	eione	F	emote -	control	
General Address Account Profile Telephones Organization Published Certificates Member Of Password Replication Dial-in Obje Member of: Name Active Directory Domain Services Folder Domain Users intra tech.nicolonsky.ch/Users Member of: Name Active Directory Domain Services Folder Domain Users intra tech.nicolonsky.ch/Users Member of: Intra tech.nicolonsky.ch/Users Intra tech.nicolonsky.ch/Users Intra tech.nicolonsky.ch/Users Users Intra tech.nicolonsky.ch/Builtin Intra tech.nicolonsky.ch/Builtin Intra tech.nicolonsky.ch/Users Ist Nicola Properties ? ublished Certificates Member Of Password Replication Dial-in Security Environment Sessions Remote Org General Address Account Profile Telephones Org Remote Desktop Services Profile COM+ Attribute Attribute Attributes:	eral Address Account Profile Telephones Organization shed Certificates Member Of Password Replication Dial-in Object nber of: ame Active Directory Domain Services Folder onain Dial-in Object ame Active Directory Domain Services Folder intra-tech.nicolonsky.ch/Users intra-tech.nicolonsky.ch/Users intra-tech.nicolonsky.ch/Users avg Admins intra-tech.nicolonsky.ch/Users intra-tech.nicolonsky.ch/Users intra-tech.nicolonsky.ch/Users avg Admins intra-tech.nicolonsky.ch/Users intra-tech.nicolonsky.ch/Users intra-tech.nicolonsky.ch/Users avg Admins intra-tech.nicolonsky.ch/Builtin Profile Dial-in account Profile Telephones Organization account Profile Telephones Organization and Address Account Profile Telephones Organization andte Desktop Services Profile COM+ Attribute Educe Attribute Educe andte Value (never) 23.11.2019 12:02:26 W. Euro andte Value 23.11.2019 00:43:09 W. Euro 00:	Remote D	eskton Ser	vices Profile	36	COM+		Attribute	Editor	
Published Certificates Member Of Password Replication Dial-in Obje Member of: Name Active Directory Domain Services Folder Domain Users intra.tech.nicolonsky.ch/Users Member of: Name Active Directory Domain Services Folder Domain Users intra.tech.nicolonsky.ch/Users Member of: Name Active Directory Domain Services Folder Domain Users intra.tech.nicolonsky.ch/Users Member of: Intra.tech.nicolonsky.ch/Users Intra.tech.nicolonsky.ch/Users Intra.tech.nicolonsky.ch/Users Users intra.tech.nicolonsky.ch/Builtin Intra.tech.nicolonsky.ch/Builtin Intra.tech.nicolonsky.ch/Builtin Set Nicola Properties ? ublished Certificates Member Of Password Replication Dial-in Security Environment Sessions Remote General Address Account Profile Telephones Org Remote Desktop Services Profile COM+ Attribute Attribute Attributes:	Address Member Of Password Replication Dial-in Object nber of: ame Active Directory Domain Services Folder one Dial-in Object ame Active Directory Domain Services Folder intra tech.nicolonsky.ch/Users one Dial-in Object ame Active Directory Domain Services Folder intra tech.nicolonsky.ch/Users one Dial-in ame intra tech.nicolonsky.ch/Users intra tech.nicolonsky.ch/Users one Dial-in actorational Services intra tech.nicolonsky.ch/Builtin Properties ? hed Certificates Member Of Password Replication Dial-in curity Environment Sessions Remote cor and Address Account Profile Telephones Organi anter Address Account Profile COM+ Attribute Econ anter Value (never) 23.11.2019 12:02:26 W. Euro 23.11.2019 00:43:09 W. Euro anter User 41 test.nicola@nicolonsky.ch CS-ConsistencyGuid \F7.40\1F\ES\28\20\4D\43 DS-KevCredentiall ink B 854-0002000020	General	Address	Account	Profile	Tel	, lenhones	Om	anization	
Member of: Name Active Directory Domain Services Folder Domain Users intra tech.nicolonsky.ch/Users Key Admins intra tech.nicolonsky.ch/Users Users intra tech.nicolonsky.ch/Builtin att Nicola Properties ? ublished Certificates Member Of Password Replication Dial-in Security Environment Sessions Remote org General Address Account Profile Telephones Org Remote Desktop Services Profile COM+ Attribute Attribute Value IastLogon 23.11.2019 12:02:26 W. Edu IogonCount attribute Value Value Value IogonCount 41 Telephones Orgon Value Telephone Value	nber of: ame Active Directory Domain Services Folder intra tech nicolonsky.ch/Users avy Admins intra tech nicolonsky.ch/Users intra tech nicolonsky.ch/Users avy Admins intra tech nicolonsky.ch/Builtin Address intra tech nicolonsky.ch/Builtin icola Properties ? hed Certificates Member Of Password Replication Dial-in curity Environment Sessions Remote cor aral Address Account Profile Telephones Organi armote Desktop Services Profile COM+ Attribute Economic armote Desktop Services Profile COM+ Attribute Economic armote Desktop Services Profile COM+ Economic fibute Value tLogonf (never) tLogon 23.11.2019 12:02:26 W. Euro attribute 41 il test.nicola@nicolonsky.ch -DS-ConsistencyGuid \F7\40\1F\E5\28\20\4D\43 DS-KeyCredentialLink B:854-000200002000019BA3	Published Cer	tificates	Member Of	Passwo	rd Rep	lication	Dial-in	Objec	ct
Name Active Directory Domain Services Folder Domain Users intra.tech.nicolonsky.ch/Users Key Admins intra.tech.nicolonsky.ch/Users Users intra.tech.nicolonsky.ch/Bailtin St Nicola Properties ? ublished Certificates Member Of Password Replication Dial-in Security Environment Sessions Remote General Address Account Profile Telephones Org Remote Desktop Services Profile COM+ Attribute Attributes:	ame Active Directory Domain Services Folder omain Users intra tech.nicolonsky.ch/Users ey Admins intra tech.nicolonsky.ch/Users intra tech.nicolonsky.ch COM+ Attribute Economic intra tech.nicolonsky.ch COM+ Attribute Economic Address Account Attribute Economic Address Account Attribute Economic Attribute Economic	Member of:								
Domain Users intra.tech.nicolonsky.ch/Users Key Admins intra.tech.nicolonsky.ch/Users Users intra.tech.nicolonsky.ch/Builtin intra.tech.nicolonsky.ch/Builtin intra.tech.nicolonsky.ch/Builtin ist Nicola Properties ? ublished Certificates Member Of Password Replication Dial-in Security Environment Sessions Remote org General Address Account Profile Telephones Org Remote Desktop Services Profile COM+ Attribute Attributes: Value IastLogon 23.11.2019 12:02:26 W. Edu lastLogon Timestamp IogonCount 41 value Value	omain Users intra.tech.nicolonsky.ch/Users ay Admins intra.tech.nicolonsky.ch/Users ay Admins intra.tech.nicolonsky.ch/Users arers intra.tech.nicolonsky.ch/Builtin icola Properties ? hed Certificates Member Of Password Replication Dial-in curity Environment Sessions Remote cor aral Address Account Profile Telephones Organi amote Desktop Services Profile COM+ Attribute Econ outes: ribute Value tLogonf (never) 23.11.2019 12:02:26 W. Euro account 41 test.nicola@nicolonsky.ch -DS-ConsistencyGuid \F7.40\1F\E5\28\20\4D\43	Name		Active Director	ry Doma	in Serv	ices Fold	er		
Key Admins intra.tech.nicolonsky.ch/Users Users intra.tech.nicolonsky.ch/Builtin st Nicola Properties ? ublished Certificates Member Of Password Replication Dial-in Security Environment Sessions Remote General Address Account Profile Telephones Org Remote Desktop Services Profile COM+ Attribute Attributes:	ey Admins intra tech.nicolonsky.ch/Users intra tech.nicolonsky.ch/Builtin intra tech.nicolonsky.ch intra tech.nicolonsky.ch	Domain Us	sers	ntra.tech.nicol	lonsky.c	h/User	s			
Users intra.tech.nicolonsky.ch/Builtin the Nicola Properties ? ublished Certificates Member Of Password Replication Dial-in Security Environment Sessions Remote of General Address Account Profile Telephones Org Remote Desktop Services Profile COM+ Attribute Attributes: Attribute Value lastLogoff (never) lastLogon 23.11.2019 12:02:26 W. Ei lastLogon Timestamp 23.11.2019 00:43:09 W. Ei logonCount 41	sers intra.tech.nicolonsky.ch/Builtin icola Properties ? hed Certificates Member Of Password Replication Dial-in curity Environment Sessions Remote cor rral Address Account Profile Telephones Organi emote Desktop Services Profile COM+ Attribute Economic nutes: nibute Value tLogoff (never) tLogon 23.11.2019 12:02:26 W. Euro attribute 23.11.2019 12:02:26 W. Euro attribute 41 il test.nicola@nicolonsky.ch -DS-ConsistencyGuid \F7\40\1F\E5\28\20\4D\43 DS-KeyCredentialLink 8:854:000200002000019843	Key Admin	s i	ntra.tech.nicol	lonsky.c	h/User	s			
tt Nicola Properties ? ublished Certificates Member Of Password Replication Dial-in Security Environment Sessions Remote of General Address Account Profile Telephones Org Remote Desktop Services Profile COM+ Attribute Attributes: Attribute Value lastLogonf (never) lastLogon 23.11.2019 12:02:26 W. En lastLogon Timestamp 23.11.2019 00:43:09 W. En logonCount 41	icola Properties ? hed Certificates Member Of Password Replication Dial-in curity Environment Sessions Remote cor ral Address Account Profile Telephones Organi emote Desktop Services Profile COM+ Attribute Ec putes: ribute Value tLogoff (never) tLogon 23.11.2019 12:02:26 W. Euro account 41 il test.nicola@nicolonsky.ch -DS-ConsistencyGuid \F7\40\1F\E5\28\20\4D\43 DS-KeyCredentialLink B:854-000200002000019B43	Users	i	ntra.tech.nicol	lonsky.c	h/Builti	in			
tt Nicola Properties ? ublished Certificates Member Of Password Replication Dial-in Security Environment Sessions Remote General Address Account Profile Telephones Org Remote Desktop Services Profile COM+ Attribute Attributes: Attribute Value lastLogonf lastLogon imestamp 23.11.2019 12:02:26 W. Ed logonCount 41	icola Properties ? hed Certificates Member Of Password Replication Dial-in curity Environment Sessions Remote cor rail Address Account Profile Telephones Organi emote Desktop Services Profile COM+ Attribute Edentication emote Desktop Services Profile COM+ Attribute Edentication enutes:									
ublished Certificates Member Of Password Replication Dial-in Security Environment Sessions Remote Seneral Address Account Profile Telephones Org Remote Desktop Services Profile COM+ Attribute Attributes: Attribute Value lastLogonf (never) lastLogon 123.11.2019 12:02:26 W. Eu logonCount 41	hed Certificates Member Of Password Replication Dial-in curity Environment Sessions Remote cor ral Address Account Profile Telephones Organi emote Desktop Services Profile COM+ Attribute Eco outes: ribute Value tLogoff (never) tLogon 23.11.2019 12:02:26 W. Euro 23.11.2019 12:02:26 W. Euro 23.11.2019 00:43:09 W. Euro onCount 41 il test.nicola@nicolonsky.ch -DS-ConsistencyGuid \F7\40\1F\E5\28\20\4D\43	t Nicola P	roperties						?	
Security Environment Sessions Remote General Address Account Profile Telephones Org Remote Desktop Services Profile COM+ Attribute Attributes: Attribute Value Value IastLogonf (never) IastLogon Timestamp 23.11.2019 12:02:26 W. Educe IogonCount 41 Value Value Value Value	Curity Environment Sessions Remote cor rail Address Account Profile Telephones Organi amote Desktop Services Profile COM+ Attribute Ed autes:									
Attribute Value Attribute 23.11.2019 12:02:26 W. Ed IastLogon Timestamp 23.11.2019 00:43:09 W. Ed	Address Account Profile Telephones Organi emote Desktop Services Profile COM+ Attribute Ecourt emote Desktop Services Profile COM+ Attribute Ecourt emote Value (never) (never) Ecourt Ecourt Ecourt Ecourt etcogon 23.11.2019 12:02:26 W. Euro 23.11.2019 00:43:09 W. Euro encount 41 test.nicola@nicolonsky.ch 41 etcosistencyGuid VF7.40\1F\E5\28\20\4D\43 Ex54:000200002000019BA3	ublished Ce	rtificates	Member Of	F Pag	sword	Replica	tion	Dial-in	(
Remote Desktop Services Profile COM+ Attribute Attributes: Value IastLogoff (never) IastLogon Timestamp 23.11.2019 12:02:26 W. Ed logonCount 41	emote Desktop Services Profile COM+ Attribute Educes: ibute Value tLogoff (never) tLogon Timestamp 23.11.2019 12:02:26 W. Euro attribute 41 il test.nicola@nicolonsky.ch -DS-ConsistencyGuid \F7\40\1F\E5\28\20\4D\43 DS-KeyCredentialLink B:854-000200002000019BA3	ublished Ce Security	rtificates Fr	Member Of	Pas	sword Sessi	l Replica	tion B(Dial-in	(
Attributes: Attribute Value lastLogoff (never) lastLogon 23.11.2019 12:02:26 W. Eu lastLogonTimestamp 23.11.2019 00:43:09 W. Eu logonCount 41	value Value ribute Value tLogoff (never) tLogon 23.11.2019 12:02:26 W. Euro tLogon Timestamp 23.11.2019 00:43:09 W. Euro onCount 41 il test.nicola@nicolonsky.ch -DS-ConsistencyGuid \F7\40\1F\E5\28\20\4D\43' DS-KeyCredentialLink B:854:000200002000019BA3	ublished Ce Security Seperal	rtificates Er Address	Member Of nvironment	f Pas	sword Sessi file	l Replica ons Teleph	tion Re	Dial-in emote c) iont
Attributes: Attribute Value lastLogoff (never) lastLogon 23.11.2019 12:02:26 W. Ed lastLogonTimestamp 23.11.2019 00:43:09 W. Ed logonCount 41	putes: ribute Value tLogoff (never) tLogon 23.11.2019 12:02:26 W. Euro tLogonTimestamp 23.11.2019 00:43:09 W. Euro onCount 41 il test.nicola@nicolonsky.ch -DS-ConsistencyGuid \F7\40\1F\E5\28\20\4D\43' DS-KeyCredentialLink B:854:00020002000019BA3	ublished Ce Security General Remote D	rtificates Er Address Jesktop Se	Member Of nvironment Account ervices Profile	f Pas Pro	sword Sessi file CC	l Replica ons Teleph)M+	tion Re iones A	Dial-in emote c Orga ttribute	(ont aniz Edi
Attribute Value lastLogoff (never) lastLogon 23.11.2019 12:02:26 W. Ed lastLogonTimestamp 23.11.2019 00:43:09 W. Ed logonCount 41	value value tLogoff (never) tLogon 23.11.2019 12:02:26 W. Euro tLogon Timestamp 23.11.2019 00:43:09 W. Euro onCount 41 il test.nicola@nicolonsky.ch -DS-ConsistencyGuid \F7.\40\1F\E5\28\20\4D\43' DS-KeyCredentialLink B:854-000200002000019BA3	ublished Ce Security àeneral Remote D	rtificates Er Address Jesktop Se	Member Of nvironment Account ervices Profile	f Pas Pro	sword Sessi file CC	I Replica ons Teleph)M+	tion Re nones A	Dial-in emote c Orga ttribute	ont aniz Edi
lastLogoff (never) lastLogon 23.11.2019 12:02:26 W. Ed lastLogon Timestamp 23.11.2019 00:43:09 W. Ed logonCount 41	tLogoff (never) tLogon 23.11.2019 12:02:26 W. Euro tLogon Timestamp 23.11.2019 00:43:09 W. Euro onCount 41 il test.nicola@nicolonsky.ch -DS-ConsistencyGuid \F7\40\1F\E5\28\20\4D\43' DS-KeyCredentialLink B:854:000200002000019BA3	ublished Ce Security General Remote D Attributes:	rtificates Er Address Jesktop Se	Member Of nvironment Account ervices Profile	f Pas Pro	sword Sessi file CC	l Replica ons Teleph)M+	tion Re ones A	Dial-in emote c Orga ttribute	ont aniz Edi
lastLogon 23.11.2019 12:02:26 W. Ed lastLogonTimestamp 23.11.2019 00:43:09 W. Ed logonCount 41	tLogon 23.11.2019 12:02:26 W. Euro tLogonTimestamp 23.11.2019 00:43:09 W. Euro onCount 41 il test.nicola@nicolonsky.ch -DS-ConsistencyGuid \F7\40\1F\E5\28\20\4D\43' DS-KevCredentialLink B:854:000200002000019BA3	ublished Ce Security Seneral Remote D Attributes: Attribute	rtificates Er Address Desktop Se	Member Of nvironment Account ervices Profile	f Pas Pro e	sword Sessi file CC Value	I Replica ons Teleph DM+	tion Rones A	Dial-in emote c Orga ttribute	(cont aniz Edi
lastLogonTimestamp 23.11.2019 00:43:09 W. Ev logonCount 41	tLogon Timestamp 23.11.2019 00:43:09 W. Euro onCount 41 il test.nicola@nicolonsky.ch -DS-ConsistencyGuid \F7\40\1F\E5\28\20\4D\43' DS-KeyCredentialLink B:854:000200002000019BA3	ublished Ce Security ieneral Remote D Attributes: Attribute lastLogoff	rtificates Er Address Þesktop Se	Member Of nvironment Account ervices Profile	f Pas Pro e	sword Sessi file CC Value (neve	I Replica ons Teleph)M+ e	tion Re A	Dial-in emote c Orga ttribute	(cont aniz Edi
logonCount 41	onCount 41 il test.nicola@nicolonsky.ch -DS-ConsistencyGuid \F7\40\1F\E5\28\20\4D\43' DS-KeyCredentialLink B:854:000200002000019BA3	ublished Ce Security Seneral Remote D Attributes: Attribute lastLogoff lastLogon	rtificates Er Address Jesktop Se	Member Of nvironment Account ervices Profile	f Pas Pro	sword Sessi file CC Value (neve 23.11	I Replica ons Teleph DM+ r) .2019 12	tion Ri nones A	Dial-in emote c Orga ttribute	(cont aniz Edi
weil test single Osiaslanduusla	il test.nicola@nicolonsky.ch -DS-ConsistencyGuid \F7\40\1F\E5\28\20\4D\43 DS-KeyCredentialLink B:854:000200002000019BA3	ublished Ce Security General Remote D Attributes: Attribute lastLogoff lastLogon lastLogon	rtificates Er Address Jesktop Se	Member Of nvironment Account ervices Profile	f Pas Pro	Sessi file CC Value (neve 23.11 23.11	I Replica ons Teleph DM+ r) .2019 12 .2019 0	tion Re nones A 2:02:26 0:43:09	Dial-in emote c Orga ttribute	(cont aniz Edi
mail test.nicola@nicolonsky.cn	-DS-ConsistencyGuid \F7\40\1F\E5\28\20\4D\43 DS-KeyCredentialLink B:854-000200002000019BA3	ublished Ce Security General Remote D Attributes: Attribute lastLogoff lastLogon lastLogon logonCour	rtificates Er Address Jesktop Se Timestamp it	Member Of avironment Account ervices Profile	f Pas Pro	Sessi file CC Value (neve 23.11 23.11 41	I Replica ons Teleph DM+ r) .2019 12 .2019 00	tion Ri A 2:02:26 0:43:09	Dial-in emote c Orga ttribute	(cont aniz Edi
mS-DS-ConsistencyGuid \F7\40\1F\E5\28\20\4D\	DS-KeyCredentialLink B:854:000200002000019BA3	ublished Ce Security Remote D Attributes: Attributes lastLogoff lastLogon lastLogon logonCour mail	Timestamp tt	Member Of Account Account ervices Profile	f Pas	Sessi file CC Value (neve 23.11 23.11 41 test.n	I Replica ons Teleph)M+ r) .2019 12 .2019 00 icola@n	tion R ones A 2:02:26 0:43:09	Dial-in emote o Orga ttribute	(cont aniz Edi ro ro



geekmania	2019
switzerland	

	Key based authentication	Certificate based authentication
Prerequisites	 At least one Server 2016 DC Server 2012 Enterprise CA Azure AD Connect 	 Windows Server 2008R2 DC'S Server 2012 Enterprise CA Azure AD Connect Azure AD App Proxy NDES Server
Choose when	 Running 2016 DC's Want to invest a minimal effort 	 Already running NDES Use other certificates with NDES
Microsoft docs	• <u>aadj-sso-base</u>	• <u>aadj-sso-cert</u>



	Key based authentication	Certificate based authentication
Prerequisites	 At least one Server 2016 DC Server 2012 Enterprise CA Azure AD Connect 	 Windows Server 2008R2 DC'S Server 2012 Enterprise CA Server 2016 ADFS Device Synchronisation Device writeback
Choose when	 Running 2016 DC's Want to invest a minimal effort 	 You love complex legacy set-ups
Microsoft docs	• <u>hello-hybrid-key-trust</u>	• <u>hello-hybrid-cert-trust</u>

AAD Join and AD authentication

geekmania switzerland 2019





Notes from the field

- AAD Connect Service Account must be in the Key Admin group
- AAD Connect member of key admin group (<u>msDs-KeyCredentialslLink</u>)
- Refresh directory scheme on AAD Connect after AD scheme extension
- CRL, CRL, CRL \rightarrow test it with certutil
 - Must be accessible from any Windows 10 WHFB client
- Use "Kerberos Authentication" template to enroll on DC's
 - Verify that domain name is addedd to the SAN
 - Check KDC in certification usage!
 - Verify key size (2048)

Hybrid Azure AD Joined devices:

• SCP entry in AD

Remove password surface:

- Disable password sign-in by policy
- Hide password sign-in credential provider from lock screen

As alternative use:

geekmania 2019

• Web-Sign-In from Lock-Screen for intial passwordless sign-in's on existing devices

Passwordless Azure AD Join and Intune enrollment:

• Authenticator with phone sign-in (needs to be preconfigured)



• Go for a WHFB deployment

Recap

- Configure SSO for on premise resource access
- Purchase devices with WHFB capabilities

Gold-Sponsor:



Silver-Sponsor:





